Mark A. Kleiman (SBN 115919)
KLEIMAN / RAJARAM
2525 Main Street, Suite 204
Santa Monica, CA 90405
Telephone: (310) 392-5455
Facsimile: (310) 306-8491
Email: mkleiman@quitam.org

Ben Gharagozli (SBN 272302)
Law Offices of Ben Gharagozli
2525 Main Street, Suite 204
Santa Monica, CA 90405
Telephone: (661) 607-4665
Facsimile: (855) 628-5517
Email: ben.gharagozli@gmail.com

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OMAR ABDULAZIZ, Plaintiff, v. TWITTER, Inc..; McKINSEY & Co.; and DOES 1-10; inclusive, Defendants,	Case No.: 3:19 CV-06694-LB ~~THIRD~~FOURTH **AMENDED COMPLAINT AND DEMAND FOR JURY TRIAL**

"We fell behind, both in our protections against social engineering of our employees and restrictions on our internal tools" Twitter CEO, Jack Dorsey acknowledging past missteps, 2020

1. This an action to vindicate the rights of Omar Abdulaziz, a political refugee who has been granted political asylum in Canada from the despotic regime in the Kingdom of Saudi Arabia ("KSA"). Because of the tremendous wealth of key figures in KSA, major corporations, including Twitter, Inc. and McKinsey & Co.[1], have enabled, collaborated with, aided and abetted, and turned a blind eye to KSA's efforts to suppress, torture, falsely imprison, terrorize, and murder dissenters both within Saudi Arabia and around the world. Twitter, Inc., and McKinsey & Co. have for monetary gain, exposed him, his family members, friends and political associates to imprisonment, torture, and even death.

PARTIES

2. Plaintiff Omar Abdulaziz (hereinafter "Plaintiff") is a graduate student and political dissident who resides in and has been granted asylum in Canada because he faced likely persecution were he to return to his native country, Saudi Arabia.

3. Defendant Twitter, Inc., (hereinafter "Twitter") is incorporated in Delaware with its headquarters in San Francisco, California. In 2011 Saudi Prince Alwaleed Bin Talal purchased $300 million worth of stock in Twitter. In 2015 Bin Talal made an additional investment, owning 5.2% of the company, more than Twitter's founder and CEO. A January 29, 2018 article in the British newspaper, *The Daily Mail* reported that after being imprisoned and perhaps tortured by KSA, Bin Talal signed over many of his assets, to Crown Prince Mohammed Bin Salman (hereinafter "MBS"). Per *The Daily Mail*, the Trump Administration allegedly made a deal with MBS allowing him to seize control of

[1] Although McKinsey & Co. was originally a named Defendant in the present matter, Plaintiff has since voluntarily dismissed without prejudice McKinsey & Co. from this lawsuit to pursue an action against McKinsey & Co. in New York. That action is currently pending: Omar Abdulaziz v. McKinsey & Company, Inc. et al. (Civil Action Number 1:21-CV_01219)

these assets and those of other princes, so long as the assets remained in the United States. Plaintiff is informed and believes and based thereon alleges that since late 2017 or January of 2018, MBS has exercised control over more Twitter stock than is owned by Twitter's founder, Jack Dorsey.

4. The true identity of each defendant denominated as a "Doe" is unknown to plaintiff at this time, so said defendants are sued in this capacity. As each such defendant becomes known to Plaintiff, he shall seek leave to amend this Complaint to set forth that defendant's true identity

JURISDICTION

General Jurisdiction over Twitter

5. Twitter's home office is in San Francisco, California, within this judicial district.

6. To the extent that the conduct giving rise to this action also implicates state law claims, this Court is requested to exercise supplemental jurisdiction over those claims pursuant to 28 U.S.C. §1367. Alternatively, diversity jurisdiction exists pursuant to 28 U.S.C. §1332.

VENUE

7. Venue is proper in this district under 28 U.S.C. §1391(b) because a substantial part of the events or omissions giving rise to this action occurred in this district.

FACTUAL BACKGROUND

8. In 2009 Plaintiff moved from Saudi Arabia to Canada after he was admitted to study at a Canadian university. While he was in Montreal as a student, Plaintiff, who is talented in the use of social media, would discuss the internal political affairs of KSA. Plaintiff would provide political commentary using Twitter and other media websites. His main contribution was criticism of the way the KSA regime ran Saudi Arabia, criticism of

the royal family in KSA, corruption of KSA, and the foreign policy of KSA. Plaintiff was especially vocal about the grave violations of human rights in KSA, KSA's disregard for Saudi citizens, and their rights and freedoms.

9. KSA has one of the worst human rights records in the world. The State Department's 2014 Human Rights Report on Saudi Arabia summarized the situation: "[H]uman rights problems reported included abuses of detainees; overcrowding in prisons and detention centers; investigating, detaining, prosecuting, and sentencing lawyers, human rights activists, and antigovernment reformists; holding political prisoners; denial of due process; arbitrary arrest and detention; and arbitrary interference with privacy, home, and correspondence. Violence against women, trafficking in persons, and discrimination based on gender, religion, sect, race, and ethnicity were common. Lack of government transparency and access made it difficult to assess the magnitude of many reported human rights problems." "The government reportedly arrested and detained multiple persons during the year, refusing for extended periods in some cases to acknowledge the detention or to provide information about an individual's whereabouts."

10. Plaintiff was also a close ally of Jamal Khashoggi who was murdered in the Saudi Consulate in Istanbul in the beginning of October 2018 by a group of assassins related to the security and intelligence services of KSA. After Mr. Khashoggi left Saudi Arabia and moved to the United States, a friendship developed between Plaintiff and Mr. Khashoggi. The two started to cooperate on a range of political activities with the objective of educating the public in Saudi Arabia. The political partnership became stronger and the two cooperated on various projects. However, most of the projects did not materialize because this partnership and friendship was suddenly cut short when Mr. Khashoggi was brutally murdered. The CIA has concluded that Crown Prince Mohammad Bin Salman ("MBS") ordered Mr. Khashoggi's assassination.

Twitter

11. Twitter informed the Securities and Exchange Commission that in 2015 it had nearly 3,900 employees and generated over $2.2 billion of yearly revenue, more than enough to put in place adequate safeguards to protect its users. Rather than maintain enough staff to protect its users, Twitter laid off 336 employees in October 15, 2015 upon Mr. Dorsey's return as CEO. This constituted 8% of Twitter's workforce. Twitter's share value increased after the lay offs. In SEC filings, Twitter's main concern is user expansion.

12. Twitter allowed two spies to operate without interference. Twitter either (1) willfully ignoring all of this because it did not want to upset KSA if it did not have to (this opportunity vanished when western intelligence agencies formally notified Twitter of the spies) or (2) did not want to invest in having human beings monitor alerts. Due to established industry standards, Twitter had infrastructure that would have set off alerts upon a Twitter employee's unauthorized access to private user data and information.

Twitter Knew or Should Have Known that the Employees Became Unfit and Hazardous and Unfit and that This Created a Particular Risk to Others, Including Plaintiff"

13. Twitter anticipated inside jobs whereby employees would, for a variety of reasons, access or attempt to access private user data. Because of this, Twitter had a "Playbook", which outlined the policies Twitter employees must obey as part of their employment. In 2013, both Abouammo and Alzabarah agreed to abide by the Twitter "Playbook." In pertinent part, the Twitter "Playbook" prohibited Abouammo and Alazabarah from engaging in outside employment or consulting "or any other business activity that would create a conflict of interest with" Twitter. Twitter's 2013 Employee Invention Assignment and Confidentiality Agreements with Abouammo and Alzabarah affirmed "a relationship of

confidence and trust" between Twitter and each employee "with respect to any information of a confidential or secret nature that may be disclosed to [them] by [Twitter]...that relates to the business of [Twitter]. It defined "Proprietary Information" to include "customer lists and data." The Employee Invention Assignment and Confidentiality Agreement further required Abouammo and Alzabarah to "keep and hold all such Proprietary Information in strict confidence and trust." As employees, Abouammo and Alzabarah promised to "keep and hold all such Proprietary Information in strict confidence and trust." They promised to "not use or disclose any Proprietary Information without the prior written consent of [Twitter]." It forbade them from using any Twitter information for any other business or employment.

14. Further, Twitter had a "Gift Policy" during Abouammo and Alzabarah's employment that stated: "[f]or gifts exceeding $100 in value, bring the gift to the attention of both your manager and VP of HR before returning to sender."

Reasons This Was Foreseeable to Twitter

15. Known as the "Arab Spring", December 2010 through 2012 saw a wave of popular protests in the Arab world against autocratic governments in the region. According to numerous social scientists and regional experts and analysts familiar with the region, social media in general and Twitter in particular was at least one of the facilitators behind the "Arab Spring." Autocratic governments, including KSA have recognized this. Since the Arab Spring, autocratic governments such as the KSA have clamped down on activists and invested heavily in state surveillance capabilities.

16. Twitter has also been used as a platform for those seeking the overthrow and/or reform of autocratic regimes outside of the Arab world, including Moldova, China and Ukraine.

17. Twitter is the 5th most frequently visited site in Saudi Arabia.

https://www.gogulf.com/social-media-saudi-arabia/ 2016 0118 last visited 2020 0824

18. Because of the use which activists have made of Twitter, authoritarian regimes in the region and throughout the world have increasingly surveilled those activists' Twitter accounts in an effort to disrupt and silence them.

19. This is especially true for Saudi Arabia. Because traditional forms of public speech are so thoroughly repressed, in the words of Plaintiff, "Twitter is our Parliament."

20. Since at least 2009 tech companies have been targets of spying attempts by authoritarian regimes. In January of 2010 Google revealed that between mid-2009 and December 2009 it had been targeted by hackers Google suspected that state actors (in this case the Chinese government) had organized an inside attack using Google's own employees in mainland China.

21. More efficient for a foreign intelligence service to bribe or coerce an employee to do an inside job than to spend tens of millions to try to hack Twitter.

22. According to Frank Montoya, the FBI's former Director of National Counterintelligence Executive, the Bureau has repeatedly warned social media platform of this well before 2015. On information and belief, Twitter, which had over 100 million users by 2012, was among the platforms so warned.

23. According to Alex Holden, Chief Executive Officer of Hold Security, new cases of

data abuse that occur every month point to carelessness among companies.

24. Twitter itself had been repeatedly hacked. On July 4, 2011 Fox News reported that

its Twitter feed had been hacked to falsely report that President Obama had been killed. On February 1, 2013 Twitter acknowledged that up to a quarter of a million user accounts had been hacked. On April 23, 2013 Associated Press' Twitter account was hacked by the Syrian Electronic Army to falsely report that there had been two explosions at the White House, and

that President Obama had been injured. The same group took over numerous Twitter domains in August 2013.

25. By the time Twitter hired Alzabarah on or about August of 2013, it had abundant notice that there was a clear and present threat of insiders being used to illegally access confidential data and that authoritarian governments such as KSA would be interested in using that data to help them target dissidents.

26. On or about June 2011, al-Qahtani publicly sought to purchase tools to ban people from Twitter or freeze their accounts.

27. On information and belief Twitter's Board of Directors was warned of the danger posed by broad access to user accounts by employees and the dangers associated with such access before Plaintiff's data was stolen and furnished to KSA by Twitter employees.

Summary of Negligence Allegations against Twitter:

28. Twitter negligently hires, trained, supervised, its employees. Twitter negligently failed to observe and control new employees it had put in risky positions and had

given great trust and authority to. Twitter negligently failed to restrict access to user data by (a) limiting the persons who had access; and/or (b) limiting the extent-duration of the access.

29. Twitter negligently failed to design, construct, implement safeguards with adequate audits and alerts.

30. Twitter negligently failed to ~~adequately~~even warn all of its users who were ~~affected~~victimized by ~~the~~this hacking that they had been hacked. Neither Plaintiff nor another extremely prominent Saudi whistle blower, Mujtahid ibn Harith ibn Hamam ("Mujtahid") received any form of

Formatted: Right: 0.33", No widow/orphan control

Formatted: Right: 0.33", No widow/orphan control

notification from Twitter that their private user information had been hacked. Both Plaintiff and Mujtahid have thoroughly searched all of their emails, including their spam folders. After conducting this diligent and thorough review of email accounts, neither Plaintiff nor Mujtahid have seen any communication from Twitter warning them that they have been hacked. Nor have either of them seen any "in-app notification" within the Twitter app itself indicating that they had been hacked despite a thorough and diligent review.

31. Twitter also negligently failed to adequately warn its users who were affected by the inside job. Although Twitter ~~claim sit~~claims it sent a notice on December 11, 2015, that notice was defective because it was vague and lacked material information it knew users would be interested to know (it did not indicate that it was an inside job, that Saudi Arabia was the state sponsor, that the victims were critics of KSA). Further, it merely stated that the users "may have" been targeted when in fact, Twitter had no reason to doubt that users were indeed targeted.

The Predictability of Attack

~~31.~~32. On November 3, 2013 Twitter hired Ahmad Abouammo as Media Partnerships Manager responsible for the Middle East and North Africa ("MENA") region. His duties included helping "notable" accounts of public interest, brands, journalists, and celebrities for the MENA region with content, Twitter strategy, and sharing best practices.

~~32.~~33. Plaintiff is informed and believes and thereon alleges that when an employee joins Twitter, he or she is supposed to apply for access to certain accounts. Grants of access depend upon the team of which the employee is a member.

~~33.~~34. Despite the sensitivity of the positions Alzabarah and Abouammo held given

political repression in the KSA and the very large number of Saudi reformers, dissidents and activists who relied upon Twitter as a platform, Plaintiff is informed and believes and based thereon alleges that Twitter made little or no effort to have an actual human security officer review or monitor the activities of Twitter employees in sensitive positions. The result of this was that although there were alerts when Abouammo and Alzabarah accessed and/or attempted to access private user data they were not authorized to access and had no legitimate reason to access, the alert fell on deaf ears and no remedial action would be taken to either stop the unauthorized access or prevent unauthorized access.

35. On June 13, 2014 a KSA official ~~emails~~emailed Abouammo with a request to verify a

~~34.~~ Saudi

Royal Family member's twitter account. On June 14, 2014, the KSA official requests Abouammo's contact information. The same day, Abouammo provides his Twitter and personal contact information to the KSA official.

~~35.~~36. On information and belief, at all relevant times, Twitter did not have a practice

or policy of periodically investigating such employees to determine whether they pose a danger to the privacy of Twitter's users. On information and belief, at all relevant times, Twitter did not have a practice or policy of periodically investigating whether employees were accessing or had accessed private user data without authorization in violation of the Twitter Playbook.

~~36.~~37. While Abouammo was at Twitter, he knew and socialized with Alzabarah. In April of 2014, Abouammo was assigned the task of helping a public relations firm, which worked for KSA to verify a newscaster's Twitter account. Abouammo then asked the public relations firm what else he could do to be of service to KSA.

~~37.~~38. Al-Qahtani was hired by the Chief of the Royal Court in Saudi Arabia to protect the KSA's reputation on-line by means of an "electronic army" suppressing adverse social media content. He was officially appointed an Advisor to the Royal Court in KSA in 2012 and given the rank of Minister in 2015. In 2018, after the murder and dismemberment of Jamal Khashoggi, al-Qahtani was relieved of his official position.

~~38.~~39. In June 2014 al-Qahtani began cultivating Twitter employees, and told Abouammo that he worked directly for MBS.

~~39.~~40. In November of 2014, al-Qahtani arranged an in-person meeting in London at a Twitter global media summit. During Abouammo's visit to London he met with Ahmed Al-Jabreen, in a face-to-face meeting, told Abouammo that he was advising a "very important" member of the Royal Family.

~~40.~~41. Al-Jabreen founded a Saudi technology company, Samaat, which has ongoing business relationships with MISK, which is an MBS-controlled multi-billion--dollar foundation, which later hired Alzabarah as its CEO.

~~41.~~42. On or about November 20, 2014, when Al Jabreen and Abouammo had both returned to the United States, they met in front of the Twitter offices in San Francisco, and remained outside of the offices for a private meeting.

~~42.~~43. On or about November 20, 2014, Al Jabreen posted a photo of himself and Abouammo in front of Twitter's headquarters.

~~43.~~44. On December 5, 2014, al-Qahtani met Abouammo in London and gave him a luxury Hublot watch valued at over $25,000.

~~44.~~45. The gift of this watch was just the first of many transactions. Abouammo

Formatted: Right: 0.26", No widow/orphan control

Formatted: Right: 0.26", No widow/orphan control

Formatted: Right: 0.26", No widow/orphan control

ultimately received at least $300,000 from KSA. In doing so, Abouammo violated the Twitter Playbook. Plaintiff is informed and believes and thereon alleges that the purpose of the Twitter Playbook's gift policy is at least in part, designed to prevent Twitter employees from being bribed into performing inside jobs for outside entities. However, because Twitter lacked the proper safeguards in place to actually investigate Abouammo, Twitter did not properly address the issue and hold Abouammo accountable.

46. Special Agent Letitia Wu, assigned to the FBI's Counterintelligence Division, furnished a sworn affidavit, which was the basis for the criminal complaint filed by the United States Attorney's Office in November 5, 2019. Agent Wu reported that "Based on information provided by Twitter and Abouammo's former supervisor at Twitter, Abouammo had no legitimate business use as a Media Partnerships Manager for accessing users' account information and doing so would have been a violation of the company's policies." Despite this, on information and belief, Abouammo had been given access to a Twitter software program which allowed him to do exactly that.

~~45.~~47. In December 2014, Abouammo began accessing private Twitter data useful to KSA often at the direct request of Al-Qahtani. On July 9, 2015~~,~~.

The Detectability of the Insider Attack at Twitter

~~46.~~48. On December 12, 2014 Abouammo began accessing private and confidential account data from the Twitter account operated by a London-based Saudi whistle blower~~,~~ Mujtahid ~~ibn Harith ibn Hamam ("Mujtahid").~~ Abouammo also accessed Mujtahid's data on January 5, 2015, January 27, 2015, February 4, 2015, February 7, 2015, February 18, 2015, and February 24, 2015. Plaintiff is informed and believes and based thereon alleges that Abouammo's illicit viewing of Mujtahid's direct messages included private communications to and from Plaintiff. Despite the alerts that were sounded in Twitter's

Formatted: Not Highlight

Formatted: Not Highlight

infrastructure due to this unauthorized access of private user data, Twitter took no remedial action in response to the unauthorized access.

~~47.~~49. At all times material hereto, Twitter's practice was to store users' direct messages for purposes of backup protection. In fact, a computer researcher reported in 2019 that "Twitter retains direct messages for years, including messages you and others have deleted, but also data sent to and from accounts that have been deactivated and suspended."

~~48.~~50. On February 16, 2015, al-Qahtani called Abouammo three times. Abouammo introduced Alzabarah to Al Jabreen. On that same day Al Jabreen called Alzabarah.

~~49.~~51. While Abouammo and Alzabarah were employed at Twitter, there were certain established industry standards with respect to service providers (including Twitter) that stored private user data. Among other things, such industry standards required a strict process of monitoring for anomalous system activity, authorized or unauthorized user access incidents (whether internal or external), and alerts as well as audits. For the alerts to be meaningful, audits and monitoring by human employees was required to actually detect and address unauthorized access of private user data. While the Twitter Playbook provided the policies for such industry standards, Twitter lacked the systems in place to actually enforce and execute those standards.

~~50.~~52. At all relevant times to this lawsuit:

a. Twitter did not have adequate access controls in place to restrict access to such sensitive data.

b. Twitter's system allowed personnel to access confidential user account information even though they were not authorized to do so.

c. Twitter was not monitoring access to this highly confidential account data or

analyzing user activity logs for this data.

d. Twitter was not utilizing tools that detect unauthorized or anomalous behavior by employees or rogue insider activities with respect to this data, or if they were, they were not receiving the reports of these tools.

e. Twitter was not restricting remote access to this sensitive account data, even by an employee who had gone absent from the workplace for a month.

f. Twitter was not enforcing its policies and confidentiality agreements.

g. Twitter had lax internal procedures regarding responses to emergency disclosure requests from an authoritarian regime.

h. Twitter's incident response procedures were lacking, since it apparently did not (a) conduct much of an internal investigation when it discovered Alzabarah's unauthorized access to the user account data or (b) engage law enforcement. It simply confronted him, put him on leave, and let him walk off to get on a plane and leave the country. This, despite Twitter having the authority and ability to detain Alzabarah and turn him over to the authorities for arrest and prosecution.

i. On information and belief, the private user account data Twitter stored was not encrypted. Had it been encrypted, Alzabarah and Abouammo would not have been able to see the account information.

j. Twitter did not have an adequate human supervision process to monitor private user data. Twitter will only be careful when there is a financial incentive for them to do so.

~~51.~~53. As further evidence, in December 2015, Twitter told the FBI that ~~they are~~it was tightening restrictions with respect to access to user information. Yet, as of the Summer of 2020, 1,000 employees and contractors have access to and can even change user data. Importantly, the FBI opened an investigation into Twitter out of national security concerns. Twitter never

learns. Some of the contractors created fake user tickets to justify or excuse the intrusion. There were so many account-spying episodes that the security team was unable to keep track of them.

~~52.~~54. It was a significant departure from Abouammo's and Alzabarah's prior practice to ~~access~~ access these accounts. Had Twitter had proper safeguards in place, they would have noticed that something was wrong and would have/should have investigated it. Neither Abouammo or Alzabarah had a legitimate reason to access these accounts. Indeed, neither Abouammo or Alzabarah's job duties included a need to access a Twitter's user's private information and doing so was a reportable violation.

55. ~~Alzabarah did not start using Profile Viewer until he started working for KSA.~~ According to Special Agent Wu's affidavit "A Twitter Security Engineer informed

~~53.~~ the FBI that, although Alzabarah may have had grandfathered access to view user information through an internal Twitter tool called 'Profile Viewer,' Alzabarah had no legitimate business purpose as a Site Reliability Engineer to access user accounts. Alzabarah's job was to help keep the site up and running, which did not involve accessing individual user accounts." This should have been a red flag for Twitter. Alzabarah's access and use of Profile Viewer would have generated an alert in Twitter's security system as an unauthorized access. Unfortunately, because Twitter lacked the monitoring in place to address such alerts, Alzabarah's unauthorized access, though easily detectable, went unnoticed and unchecked.

~~54.~~56. In the exercise of due care any and all of Abouammo and Alzabarah's unauthorized access escapades should have been detected and been cause for intervention.

Formatted: Normal, No bullets or numbering

Formatted: Font: 9 pt, Italic, Not Highlight

~~55.~~57. On February 20, 2015, Al Jabreen tweeted a photograph of himself with Alzabarah.

~~56.~~58. On March 8, 2015, Abouammo sent al-Qahtani a direct message via Twitter proclaiming, “proactively and reactively we will delete evil, my brother".

~~57.~~59. Alzabarah tells his wife on a Twitter owned laptop that he is going to Washington at the request of KSA

~~58.~~60. On May 13, 2015, Al Jabreen posted a photo of himself with MBS, exclaiming that he was honored to meet the dictator.

~~59.~~61. On the very next day, Alzabarah flew from San Francisco to Washington, D.C., where he stayed only twelve hours, to meet with representatives of MBS before returning to California.

~~60.~~62. KSA recruited Alzabarah to access Plaintiff’s private Twitter information (e.g. direct messages and other confidential data and information that is not available to the public) and leak it to KSA.

63. ~~Beginning on May 21~~Less than one week after Alzabarah’s clandestine trip to meet a high ranking Saudi official, he began hacking into the private user information of Twitter account holders. Literally the first account he hacked was Mujtahid’s. Mujtahid is identified as User-1 in the affidavit signed by Special Agent Wu.

64. Mujtahid’s account was repeatedly hacked. Alzabarah was able to view his true email address and telephone number, along with other private information.

Formatted: Not Highlight

65. On or about September 27 and September 28, 2015, while Alzabarah was actively hacking into the private user information of Twitter account holders, Mujtahid's entire Twitter account, including his cache of direct messages, was taken over by Saudi operatives.

66. On September 28, 2015, Mujtahid filed a formal complaint with Twitter, reporting that his private information had been illegally accessed.

67. ~~and continuing~~Prior to the hacking of Mujtahid's account information, Plaintiff had relied upon the supposed security of Twitter's direct messaging function to share with Mujtahid information he had obtained from highly placed sources in Saudi Arabia. The DMs between Plaintiff and Mujtahid exposed to MBS and KSA that Plaintiff had access to a network that was giving Plaintiff confidential information that was politically damaging to MBS. Plaintiff and Mujtahid also discussed the infighting between MBS and his royal rival, Prince Muhammad bin Nayef, which at the time, was not publicly known. Plaintiff and Mujtahid were also arranging some hashtags and campaigns that would have been politically damaging for ~~approximately~~MBS and KSA. Plaintiff and Mujtahid were also discussing infighting among certain KSA princes, who were subsequently jailed for criticizing MBS. Twitter's lackluster security allowed Alzabarah to access DM's between Plaintiff and Mujtahid, which in turn alerted KSA and MBS that Plaintiff had access to a sensitive network of individuals who were providing Plaintiff with private information about KSA and MBS that was not otherwise accessible and was also politically and personally damaging for KSA and MBS.

68. In December 2015, individuals from this sensitive network that was providing Plaintiff with private and damaging information about MBS and KSA were jailed in order to be silenced. However, since they had already provided information to Plaintiff, MBS and KSA knew that the private and damaging information was still out there and the only way to stop it from leaking further was to silence Plaintiff. One prince has not been heard from since December 2015.

Formatted: Not Highlight

Formatted: Not Highlight

~~61.~~ In the next six months~~,~~

69. Alzabarah ~~accessed~~hacked the confidential user data for nearly 6,000 Twitter users, including at least 33 names for which KSA security personnel had asked Twitter for "emergency disclosures." Alzabarah had no legitimate reason to access private user information. Granting Alzabarah unnecessary access to so many accounts over such a long period of time is a glaring failure under established industry standards. Indeed, the established industry standards provide that an employee must apply for access to private user data. Had Twitter been following those standards, Alzabarah would not have been able to access the private user information that he did access because he had no job related purpose to do so. Since he did not need to do this for his job, he would have had to apply for permission to do so and his application would have been denied. Further, such established industry standards indicate that even where an employee receives access to private user data after providing good cause for such access in an application, such access is only granted for a very limited period of time and 6 months vastly exceeds any established industry standards.

~~62.~~70. To accomplish this, Alzabarah used official Twitter software called a Profile Viewer. This Twitter software, along with other company tools, afforded Alzabarah access to private account information. Plaintiff is informed and believes and based thereon alleges that the account information that could be viewed by Profile Viewer and other means available to Alzabarah included but was not limited to information about the devices the account holder used, all recent IP information, logs containing the user's actions on Twitter, including direct messaging, logs containing information about the browsers used by the account holder, and all holder-provided biographical information.

~~63.~~71. On May 22, 2015, the day after Alzabarah began his illegal searches, Abouammo resigned from Twitter. On information and belief, Abouammo left Twitter having had unauthorized access for about 5 months and nobody at Twitter ever confronted him about it.

Formatted: Right: 0.2", No widow/orphan control

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

~~64.~~72. The aberrant conduct of Abouammo and Alzabarah constituted "red flags" which did set off alerts to Twitter of illegal and unauthorized activity. Twitter disregarded facts which rendered Abouammo and Alzabarah unfit for continued employment in a sensitive position which allowed him to access confidential user data.

~~65.~~73. On or about May 29, 2015, Alzabarah accessed, without authorization, private account information of two Twitter accounts over the course of approximately one hour.

~~66.~~74. Long after Abouammo had left Twitter, he continued contacting his former colleagues to transmit KSA security officials' requests for private information about Twitter account holders. Although Twitter managers asked him to stop, and to direct Saudi officials to contact Twitter directly. Abouammo continued to handle this personally. This also should have prompted Twitter to investigate what Abouammo had done while he was at Twitter.

~~67.~~75. In June of 2015 Alzabarah accessed private and confidential information from 5,726 Twitter accounts in violation of established industry standards. Unauthorized access to so many accounts in such a short period of time would have sent alerts to Twitter's security system. However, because there was insufficient monitoring, the alerts went ignored.

~~68.~~76. The private confidential information Plaintiff had trustingly left in Twitter's care included his unique and complex Twitter password, his IP addresses, and his direct messages, none of which Plaintiff had shared with the public or with KSA.

~~69.~~77. With the first month of raiding undetected by Twitter, on July 5, 2015 Alzabarah

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

again accessed Plaintiff's confidential and private information.

~~70.~~78. To his knowledge and recollection, Plaintiff has never even met Alzabarah or Abouammo, and neither bears any personal malice towards Plaintiff.

~~71.~~79. Plaintiff had placed his full trust and confidence into Twitter that his data and anonymity with respect to his pseudonymous account would be protected. Twitter breached that duty to him by allowing two employees to do what Twitter had promised Plaintiff would not happen: gain unauthorized access to his private user data and violate his privacy. Importantly, on information and belief, Abouammo and Alzabarah raided both Plaintiff's regular account and pseudonymous account.

~~72.~~80. Nonetheless, the danger Alzabarah and Abouammo posed to Plaintiff's confidential

data was inherent in Twitter's manner of operation. First, Twitter furnished Alzabarah and Abouammo with the access, hardware and software tools that enabled them to raid Plaintiff's private information. This would not have been possible were they not employed by Twitter. Second, Twitter implemented and benefited from policies that allowed and encouraged its technical and professional staff to work offsite, from multiple locations. Although Twitter benefitted from the greater productivity this allowed, it even further reduced Twitter's ability to monitor sensitive employees' conduct. Finally, Twitter implemented and benefitted from policies allowing its professional and technical staff flexibility as to when and where they performed their work, further complicating any monitoring Twitter should have been doing. With hundreds of millions of active users and a great many employees who had access to their data, the risk that confidential data would be exposed was broadly incident to Twitter's mode of operation.

~~73.~~81. Despite all of the known risks that the private information of account holders was in

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

danger, Twitter failed to institute adequate safeguards to protect this data or even alert Twitter's senior management that private account data was being raided.

~~74.~~82. In 2015, Twitter's terms of service contained a privacy policy. Twitter informed its users (including Plaintiff) by way of its privacy policy effective May 18, 2015 that "Our default is almost always to make the information you provide through the Twitter Services public for as long as you do not delete it, but we generally give you settings or features, like direct messages, to make the information more private if you want." Twitter, due to the herein alleged conduct, has breached the terms of service and privacy policy.

~~75.~~83. On or about June 19, 2015 and July 2015, Alzabarah accessed Plaintiff's account.

~~76.~~84. Just weeks after the massive invasion of Twitter accounts, Alzabarah took an entire month of personal leave, beginning July 11, 2015. He immediately flew to Saudi Arabia. While on personal leave in Saudi Arabia he broke into the private and confidential information of hundreds of other Twitter account holders. Inexplicably, Twitter permitted this and never confronted him over this until December 2, 2015 after Twitter was informed of Alzabarah's criminal activity by Western intelligence agencies.

~~77.~~85. On or about September 27 and 28, 2015, Alzabarah without authorization accessed Mujtahid's private information.

~~78. On September 28, 2015, Mujtahid, the London-based whistle-blower filed a formal complaint with Twitter, reporting that his private information had been illegally accessed.~~

~~79.~~86. Despite being uniquely qualified and situated to discover the herein alleged

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Not Highlight

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

breaches of confidential data, Twitter was either unaware of Abouammo's and Alzabarah's activities or chose to not investigate them until it was notified by Western intelligence officials. On December 2, 2015, Twitter confronted Alzabarah with this information and placed him on administrative leave. On information and belief, Alzabarah left Twitter having enjoyed unauthorized access for about 6 months and nobody at Twitter had ever confronted him about it until Twitter was notified by Western intelligence agencies in December 2015.

~~80.~~87. The very next day Alzabarah, his wife, and his daughter fled the country after numerous telephone calls between him and the Saudi Consulate in Los Angeles. Alzabarah resigned from Twitter while flying out of the United States on December 3, 2015.

~~81.~~88. Neither Alzabarah or Abouammo made any attempt to conceal their illicit activities while at Twitter.

~~82.~~89. Twitter failed to follow FBI recommendations to report foreign travel, report foreign

contact, etc. Had Twitter followed these guidelines, they could have stopped Alzabarah and Abouammo

~~83.~~90. ABOUAMMO and ALZABARAH had access to proprietary and confidential ~~Twitter~~

Twitter information, including information about Twitter users, such as the user-provided names and birthdates, device identifiers, relationships, phone numbers, internet protocol ("IP") addresses and session IP histories, among other things.

~~84.~~91. Neither ABOUAMMO's nor ALZABARAH's job duties involved a need to access ~~a~~

a Twitter user's private information and doing so was a reportable violation of the Twitter Playbook policies regarding handling and protecting user data.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Right: 0.26", Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Right: 0.26"

Formatted: Right: 0.26", Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Right: 0.26"

~~85.~~92. Neither ABOUAMMO nor ALZABARAH had authority from Twitter to receive, access, or produce user information pursuant to any governmental emergency disclosure request.

~~86.~~93. Even after Alzabarah left the country, Abouammo continued to use his internal networks to gather information inside Twitter. Abouammo continued to do this until at least March 1, 2016. There is no indication from Twitter that it has plugged these leaks.

How the Twitter Inside Job Harmed Plaintiff

~~87.~~94. The Profile Viewer software that Twitter let Abouammo and Alzabarah use allowed them to access private user account data, on both Plaintiff's public account and a pseudonymous account Plaintiff established so he could help people who might be afraid to be in touch with him directly. The data illicitly viewed by the Twitter employees exposed Plaintiff's name on the pseudonymous account, his IP address, his password, his direct messages, and his telephone number. Neither Abouammo or Alzabarah had any legitimate reason to be using the Profile Viewer software and doing so would have sent an alert to Twitter's security systems. The importance of the breach of Plaintiff's pseudonymous account cannot be understated as Plaintiff's pseudonymous account was more significant for his activism than Plaintiff's regular Twitter account. Had Twitter had adequate security, KSA and MBS would have never learned that Plaintiff was operating this particular pseudonymous account.

95. Shortly after Mujtahid's DMs were raided the hacker used Mujtahid's direct messaging capability to send a DM to Plaintiff saying, "You're next, motherfucker."

96. In addition to revealing Plaintiff's extensive network of highly placed informants

Formatted: Right: 0.26", Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Right: 0.26"

Formatted: Right: 0.26", Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

within Saudi Arabia, Alzabarah's hack of Mujtahid's DMs exposed extensive discussions about other matters which caused MBS to focus on Plaintiff and single him out for surveillance, harassment, and intimidation through the imprisonment and torture of his family members. Specifically, Alzabarah obtained information showing that:

(a) Plaintiff was in regular contact with numerous public figures and political activists;

(b) Plaintiff had obtained insider knowledge about the political struggle between MBS and then Crown Prince Muhammad bin Nayef;

(c) Plaintiff had obtained insider knowledge about other princes who were contesting MBS' bid for the throne; and

(d) Plaintiff and Mujtahid were closely collaborating on campaigns to mobilize Twitter opposition to MBS and his political positions.

97. Prior to Alzabarah's hack of Mujtahid's DMs, MBS had no knowledge of the central role Plaintiff was playing in generating political opposition to MBS that went beyond the level of open-source information. Subsequent to Alzabarah's hack, MBS and KSA became aware that Plaintiff was capable of actually causing political damage to MBS and KSA with the private information that Plaintiff had obtained. Specifically, this information pertained to the fighting between MBS and Nayef and other princes who were fighting over the throne. As mentioned previously, this information was confidential.[2]

---

[2] To protect the safety of Plaintiff and others, further details regarding the private information that Plaintiff obtained are not listed here. Specifically, Plaintiff's correspondents have expressed such fear and concern about their safety that they were unwilling to give Plaintiff permission to file direct messages that they had with Plaintiff. Even though Plaintiff offered his correspondents anonymity, their fear and concern of exposure were direct messages to be quoted were so great that even correspondents whose messages had been preserved by Plaintiff were unwilling to permit their disclosure.

~~88.~~98. Plaintiff relied upon Twitter promise that the direct messages (DMs) would remain private to help protect his allies, associates and those who merely sought to correspond with him but feared KSA retaliation were the relationship with Plaintiff were to become publicly known. Some Twitter users in Saudi Arabia used direct messaging to ask Plaintiff to express analyses or opinions they were afraid to publicly express themselves. The privacy direct messaging offered was essential for conversations Plaintiff had with dissidents and activists who would be endangered were the authoritarian regime to learn of their beliefs.

99. In addition to Plaintiff's DMs with Mujtahid that were revealed to MBS, Plaintiff ~~89.~~ is informed and believes and based thereon alleges that Abouammo and Alzabarah raided and furnished to KSA included conversations with other dissidents and activists that Plaintiff wished to keep private and out of the public realm because of the sensitive nature of those conversations (relying upon Twitter's privacy policy) out of concern that if such conversations became public, Plaintiff would be harmed given the nature, content and individuals involved in those direct messaging conversations.

100. ~~90.~~ On information and belief, Twitter records and preserves geolocation data on its users, even those using the supposedly private DM system. Geolocation data of DM users made the users in Saudi Arabia vulnerable to surveillance and imprisonment. On information and belief Twitter has denied that there are data logs which would show that Plaintiff's DMs had been accessed. However, when Plaintiff refused demands that he return to Saudi Arabia KSA unleashed a brutal campaign upon a great many of people who

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

had done nothing more than privately correspond with Plaintiff, arresting and imprisoning a great many of them within days of one another.

~~91.~~101. Twitter employees Abouammo and Al-Zabarah also used Twitter software to obtain the IP address of many of their victims, including Plaintiff. At the time Plaintiff's private user Twitter data was stolen he had two tablet computers which he frequently used from his home. Compromising an IP address greatly aids in locating people who frequently use a particular router. Indeed, that Plaintiff's public and pseudonymous accounts used the same static IP address would greatly aid any surveillance team in determining that both Twitter accounts may be operated by the same person.

~~92.~~102. The value of knowing an IP address is apparent from the fact that Citizen's ~~Lab,~~ Lab, the NGO dedicated to protecting human rights through internet security was able to locate and identify Plaintiff as the first victim of the Saudi's Pegasus malware attack by tracing aberrant data traffic patterns to a particular static IP address.

~~93.~~103. Twitter employees Abouammo and Alzabarah also used Twitter software to ~~obtain~~ obtain Plaintiff's telephone number. Access to this number enabled KSA to send the malware to Plaintiff's phone via a spear-phishing text message.[3] Neither Abouammo or Alzabarah had any legitimate reason to access this private information from Twitter's database and doing so would have sent an alert to Twitter's security systems.

[3] In 2013 when Plaintiff was 22 he gave his phone number to someone who posted it to the Facebook page of a Montreal film making group-, as Plaintiff was looking for assistance in making a YouTube series about immigrants. Although Twitter argues that its Saudi investors could have learned of his telephone number this way, this unproven assertion is a matter for discovery, not resolution at the pleading stage.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Right: 0.33", Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75", No widow/orphan control

Formatted: Right: 0.33", No widow/orphan control

Formatted: Font: 9 pt

~~94.~~104. The information Twitter's employees stole and turned over to KSA was essential to MBS' plan to silence Plaintiff by threatening, and ultimately imprisoning and torturing his brother, his friends, and even just people who had exchanged messages with him on Twitter. Plaintiff's family had never been threatened until late in December 2015 or the first weeks of 2016, immediately after Alzabarah returned to Saudi Arabia to take his executive position in MISK.

~~95.~~105. The interrogation of Plaintiff's family in early 2016 was followed by the imprisonment of his brothers and torture in 2018. Tragically, they are far from the only people to suffer in this manner. In March of 2018, just months before Plaintiff's brothers were seized, Areej al-Sadhan, who had only used an anonymous account to Tweet his criticisms of MBS, was among those swept up by Saudi police. Gamal Eid, executive director of the Arabic Network for Human Rights Information, or ANHRI, an Egypt-based group that monitors human rights violations in the region is emphatic that the timing of the arrests of five other Saudi critics who had used anonymous Twitter accounts shows that the arrests are linked to the data stolen by the two Twitter employees. That data has allowed KSA to hunt down and persecute dissenters.

~~96.~~106. Control over Twitter was actually a point of pride for MBS. In 2015 MBS had bragged to Dr. Saad that MBS had had "our guy in Twitter" stop someone, which Dr. Saad understood to mean that a Twitter employee was covertly working for MBS. In 2017 al-Qahtani, who had previously sought software that could be used to either ban Twitter users

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

or to repeatedly freeze their accounts, boastfully tweeted, "Does a pseudonym protect you from the black list? No."[4]

~~97.~~107. Beginning in 2014 and through 2015, there were two Saudi spies in Twitter's ~~employ~~ employ raiding private user data for the benefit of the Kingdom of Saudi Arabia (KSA). The FBI subsequently learned about this. In late 2015, while one of the Saudi spies was still working at Twitter, the FBI met with Twitter lawyers and let them know that they had a mole, Alzabarah. They informed Twitter that Alzabarah had used his Twitter position and Twitter software to obtain private user data, and that thousands of accounts had been breached. The FBI explained that the situation was sensitive, the investigation was at an early stage, and expressly asked Twitter to not tell Alzabarah what was going on as it could hurt the case if he found out about the investigation.

~~98.~~108. Twitter refused to comply with the FBI's simple request. Instead, Twitter confronted Alzabarah with accusations that he had improperly accessed user accounts. Alzabarah readily admitted that he had accessed the information. Despite having the legal authority to arrest Alzabarah on the spot pursuant to California Penal Code § 837 so that the FBI could at least come to the headquarters and arrest him, Twitter escorted him out of the building and suspended him. Alzabarah then immediately made arrangements to escape the United States and resigned from Twitter.

~~99.~~109. Justice Department officials were livid as Twitter had blown up their case by

Formatted: Right: 0.26", Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Right: 0.26"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

[4] It is a measure of KSA's control over Twitter that even this direct threat of government violence against other Twitter users did not lead to even a brief suspension of Al-Qahtani's account. It would be another two years before he was finally banned from the platform.

tipping off a man they were hoping to arrest. Since Alzabarah had left the country and returned to Saudi Arabia, he was out of reach of American law enforcement agencies. Although charges have been brought against Alzabarah, he will likely never be held accountable because KSA will not send him back to the United States for prosecution.

~~100.~~110. Twitter knew that Alzabarah had been working for KSA. By October of 2015 the Saudi Royal Family owned more of Twitter's stock than did its founder and CEO, Jack Dorsey. In April of that year Twitter's share value had plunged 18% after a poor first quarter 2015 performance. Twitter had every reason to downplay this major security breach, and to avoid antagonizing its largest investors. And so it did.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

~~101.~~111. Twitter inexplicably waited at least nine days from the time government agents told Twitter of this massive insider job before breathing a word to anyone outside the company. There was no press release the way other data breaches were admitted. There was no repudiation of KSA spying. In fact, there was no mention of KSA at all.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

~~102.~~112. Nine days after bidding Alzabarah farewell Twitter quietly sent emails and in-application notices to some -- but not all -- of the victims. ~~Plaintiff and another prominent London-based dissident using the name Mujtahid, received no warning at all.~~Neither Plaintiff nor Mujtahid received any form of notification from Twitter that their private user information had been hacked. Both Plaintiff and Mujtahid have thoroughly searched all of their emails, including their spam folders. Neither have seen any communication from Twitter warning that they have been hacked. Nor have either of them seen any "in-app notification" within the Twitter app itself indicating that they had been hacked. On information and belief, Twitter gave no notice to the popular press -- and did not even notify

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Not Highlight

the "tech for laypersons" media such as CNET or Wired. News of the theft filtered out in an extremely circumscribed way in a few technical publications, and only because some security researchers who were among the victims blogged or Tweeted about it. Twitter did not tweet about it nor did it hold a press conference.

~~103.~~113. Twitter's tight-lipped and cryptic warning was useless. Twitter never told a soul that the Saudis, their investors, had done this. Instead, Twitter merely cautioned that a "state actor" ***might*** have been involved, leaving victims utterly in the dark about whether the data had been stolen by China, Russia, or any other nation. This was so mysterious Runa Sandvik, a security researcher who used to work for the Tor Project and now trains journalists in privacy and security criticized the notice as "not terribly helpful", telling a technology reporter that it gave her no information about who it was or what had flagged Twitter's suspicions. What is more, there were no clear links between the users who did receive the December 11, 2015 notice. Overall, the Twitter users who did receive the December 11, 2015 notice were just left confused and with more unanswered questions about what had even happened.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

~~104.~~114. Far from a full-throated repudiation of this massive theft, Twitter said nothing of the Saudi role. It did not want to upset its KSA investors. Twitter's December 11, 2015 notice did not redress the harm done by its employees: Abouammo and Alzabarah.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

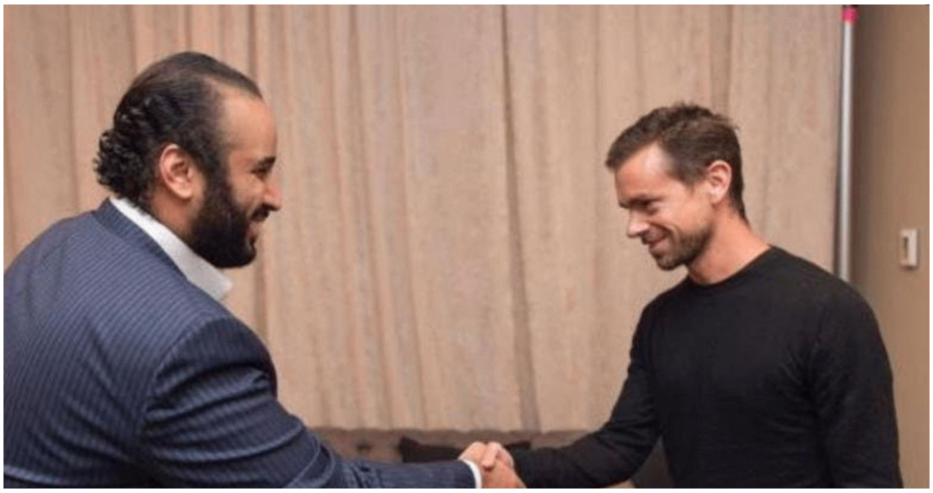
~~105.~~115. Just one month after being caught, Alzabarah began using an email address showing his affiliation with the multi-billion dollar MISK Foundation, of which he is now the Chief Executive Officer. MISK is MBS's personal foundation and Al-Qahtani sits on its Board of Directors. If Twitter had indeed been investigating Alzabarah after his resignation,

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

they would have discovered this fact and should have warned the victims about it as it further evidenced that KSA had been behind the attack (the regime rewarded the Twitter spy with a prestigious and presumably lucrative job).

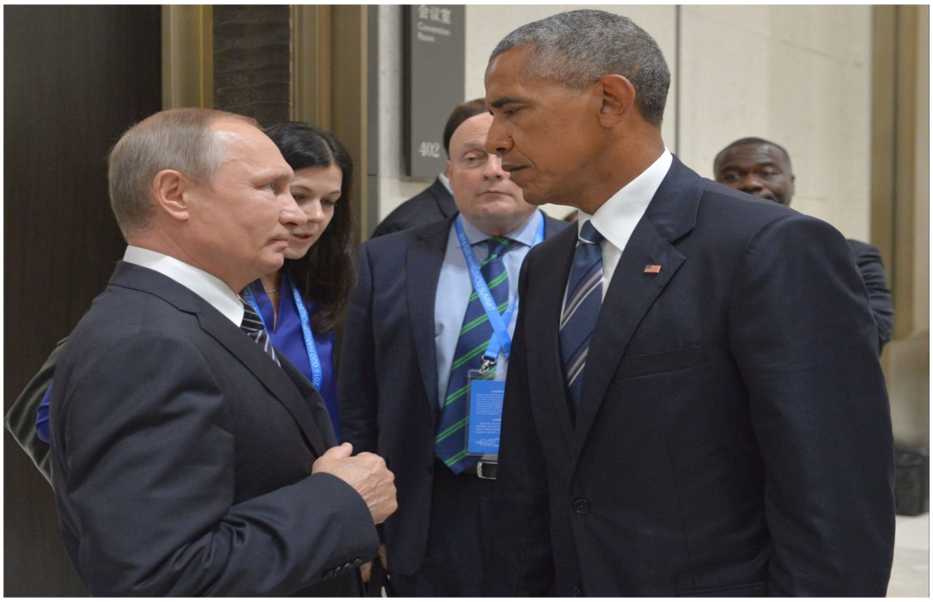
~~106.~~116. In the six months after Alzabarah fled, Twitter's CEO, Jack Dorsey, met with MBS, despite knowing full well that Alzabarah and Abouammo had pillaged Twitter accounts on behalf of KSA and knowing that MBS rewarded Alzabarah by making him CEO of MISK. Mr. Dorsey did not forget to bow his head to the dictator who had been behind the raid of private information of his platform's users.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"



~~107.~~117. Mr. Dorsey's subservience starkly contrasts with the behavior one may expect from an executive whose institution has been mistreated:

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"



~~108.~~118. Twitter never revealed to the Plaintiff or the numerous other victims of this data theft that the company derived great financial benefit from its relationships with KSA, other despots in the region, and millions of individuals living in Saudi Arabia.

~~109.~~119. Twitter also insisted on retaining the financial benefits of those relationships despite the irreversible damage done to so many of its account holders.

~~110.~~120. Twitter was so tolerant of Saudi misconduct that it did not even begin canceling the fake Twitter accounts of Saudi bots until 2019, thus continuing in its pattern of avoiding taking any action that would protect users but upset KSA until it could not delay any further.

Twitter's December 11, 2015 Notification Went to Only Some of the Victims. Plaintiff and Another Leading Saudi Dissident Were Strangely Excluded.

~~111.~~121. On December 11, 2015 Twitter sent out a "safety" notice to the owners of some of the accounts whose data had been ransacked. The notice did not explain why Twitter had delayed at least nine days in notifying them.

~~112.~~122. In addition to claiming it sent an email notice which at least Plaintiff and Mujtahid had never received, Twitter also claims that it sent an "in app" notice, complete with an "Acknowledge" button for recipients to click. Tellingly, although Twitter has furnished the Court with what it purports to be a list of recipients of the email notice, it has never furnished anything to suggest that Plaintiff either received this "in app" notice or had acknowledged it. Although Twitter claims to have sent this material, Plaintiff has not been allowed to conduct discovery to test Twitter's claim. It is important to note that according

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

to at least one article published on August 18, 2020, only a few dozen individuals received the December 11, 2015 notice. According to the Guardian, Twitter sent the December 11, 2015 notice to more than 20 users. The December 11, 2015 notice also claims that there were only a small number of accounts that "may have" been targeted.

Formatted: Not Highlight

The December 2015 Notice Was False and Misleading

~~113.~~**123.** The notice Twitter claims to have sent Plaintiff included the following: "As a precaution, we are alerting you that your Twitter account is one of a small group of accounts that may have been targeted by state-sponsored actors". Neither Plaintiff nor Mujtahid ever received this safety notice and, upon information and belief, alleges that Twitter never sent Plaintiff of Mujtahid this safety notice. Nor did Twitter ever inform Plaintiff that the individual who targeted the accounts were working for KSA, or that KSA was so intent upon getting the data that it had gone to the trouble of recruiting Twitter employees to spy on him. Nor did Twitter say that it was an inside job or what that the victims had in common (critics of KSA). Twitter further tried to water down the notice by saying the recipients "may have" been targeted when in fact, Twitter had no reason to doubt that the raid of the information had actually happened. Further, Twitter never updated the recipients of the notice. Twitter also lied in the notice when it said "At this time, we have no evidence they obtained your account information, but we're actively investigating this matter. We wish we have more we could share, but we don't have any additional information we can provide at this time." In fact, Twitter did have additional information beyond what was contained in the notice (e.g. that it was KSA behind the attacks, that it was an inside job, the victims had commonalities in that they were critics of KSA). On information and belief, Twitter deliberately chose not to share this information with the

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

recipients because Twitter knew that if it did so, it would become public, would upset KSA and hurt Twitter's bottom line. Twitter chose money over the safety of its users and complying with notice requirements in the event of a breach.

Formatted: Font: Not Bold

Twitter's Notification Process and Twitter's Ongoing Disinterest in Security Makes This Certain to Recur

~~114.~~124. If Twitter had told Plaintiff the truth he would have taken additional precautions. He could have gotten a new phone and new phone number. Or he would have become much more careful about clicking on hyperlinks embedded in text messages unless he personally knew the sender and was confident that the text message came from the sender. Plaintiff thus would not have clicked on the link on the text message that falsely purported to be from the package delivery service (which is what allowed KSA to hack Plaintiff's phone using Pegasus malware).

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

~~115.~~125. Twitter's disdain and/or apathy for the security of its user's information continues to this very day. In December 2015 Twitter claimed to the FBI that it had "enhanced its controls and permissions to restrict access to user information only to those whose duties require access." Yet in the wake of the recent hacking of 130 Twitter accounts including those of Barack Obama, Joe Biden, Elon Musk, Jeff Bezos, Michael Bloomberg, and Bill Gates, it has been revealed that over one thousand Twitter employees and off-site contractors had routine access to private user information. Pursuant to the established industry standards, this constitutes too many people with access.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

~~116.~~126. According to former security employees, Twitter management has often dragged its heels on upgrades to information security controls, while prioritizing consumer products and features, a source of tension for many businesses.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

~~117.~~127. Efforts to control Twitter's user-support staff and contractors have also gotten short shrift, according to the former security employees who said that the security of users' private data was not a major concern for Twitter executives. A former FBI cyber and cryptocurrency investigator, Patrick Westerhaus has warned that tech companies' "hyper-focus on growth and revenue" eclipses concerns for security. On information and belief, this includes Twitter.

~~118.~~128. In doing the things herein alleged Twitter consciously disregarded the rights of Plaintiff and of hundreds, if not thousands of other dissidents. Twitter knows dissidents have depended upon it to host their sensitive communications.

Plaintiff's Claims Against Twitter are Timely

~~119.~~129. Plaintiff did not receive even the weak and unhelpful December 11, 2015 notification in any way. He ~~did receive~~only received the February 17, 2016 notification that his data may have been viewed "by another user~~", however this~~".

130. Plaintiff was completely unaware of Twitter's claim that Twitter sent him the December 11, 2015 notice ~~had nothing~~until Twitter moved to ~~do with the KSA inside job.~~ dismiss.

131. Neither notice even hinted that KSA had engineered an inside job. Neither notice even hinted that the Saudi government had stolen ~~his~~Plaintiff's data ~~by way of an inside job at Twitter~~. He first learned of this on October 20, 2018 when this data theft was revealed in the New York Times. Until that day he did not know, and could not, in the

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Font: Bold, Underline

Formatted: Right: 0.33"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

exercise of reasonable diligence, be expected to know that the Saudi government had recruited and bought off two Twitter employees, who had been specifically instructed to get his private user data. Nor did he know, and could not have been expected to know that the Twitter employees had accessed his data because the company had let them use software they could use for this purpose even though, in the words of the Department of Justice, "Neither Abouammo's nor Alzabarah's job duties included a need to access a Twitter user's private information~~." .~~."

The Predictable Consequences of Twitter's Misconduct

~~120.~~132. Up to the time Plaintiff applied for asylum in Canada in 2013, KSA had stopped paying his salary and cancelled his scholarship. He was afraid that if he returned to Saudi Arabia, he would be persecuted (e.g. imprisoned, tortured or killed). However, his family remained unharmed and free from harassment, arrest, imprisonment and persecution from KSA. Upon applying for asylum in Canada in 2013, Plaintiff was not concerned that KSA would persecute his family and friends in Saudi Arabia or send a hit team to murder Plaintiff in Canada.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

~~121.~~133. After defendants' misconduct KSA's persecution of Plaintiff intensified to an unprecedented level.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

~~122.~~134. After Alzabarah improperly spied on Plaintiff's confidential Twitter data, he fled the United States on December 3, 2015. Within a month after Alzabarah fled, KSA interrogated Plaintiff's father and brother in Saudi Arabia, and cancelled Plaintiff's brother's financial assistance. KSA then and summoned three of Plaintiff's friends and roommates in Canada to the Saudi Cultural Bureau between March 2016 and July 2016. KSA had never targeted or pressured Plaintiff in this way before December 2015. Apart from Twitter

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

allowing KSA spies to access Plaintiff's private user data and furnish it to KSA, nothing out of the ordinary had happened in 2014 or 2015 to have triggered this escalation of persecution beginning in December 2015. Before December 2015, the most KSA had done to Plaintiff was cancel his salary and his scholarship. By the time Plaintiff applied for asylum in Canada in 2013, KSA had stopped paying his salary and cancelled his scholarship. Although he was afraid that if he returned to Saudi Arabia, he would be persecuted (e.g. imprisoned, tortured or killed), Plaintiff felt entirely safe in Canada. Further, his family remained unharmed and free from harassment, arrest, imprisonment and persecution from KSA. Upon applying for asylum in Canada in 2013, Plaintiff was not concerned that KSA would persecute his family and friends in Saudi Arabia or send a hit team to murder Plaintiff in Canada.

~~123.~~135. KSA received an enormous amount of stolen private user data from its loyal Twitter employees. Plaintiff is informed and believes and thereon alleges that it would have taken many months if not years for KSA intelligence members to review and analyze the data to determine who they would target.

~~124.~~136. KSA kept the data until they were able to target Plaintiff directly (when Pegasus became available and operational to them as described below).

~~125.~~137. Plaintiff is informed and believes and thereon alleges that although Abouammo Alzabarah invaded thousands of Twitter accounts of Saudi dissidents, KSA elected to use Pegasus malware to target only a relative few, including Plaintiff. Apart from himself, Plaintiff is ~~unaware~~aware of ~~other Twitter users~~ only four individuals who KSA targeted with Pegasus malware~~.~~ (three were Twitter users and one was a high-ranking former Saudi government official-Dr. Saad Aljabri). Plaintiff is informed and believes and thereon alleges that KSA targeted Plaintiff with Pegasus malware because of what KSA learned from

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

accessing Plaintiff's Direct Messages on Twitter's platform that Alzabarah and Abouammo wrongfully accessed and furnished to KSA while Alzabarah was employed at Twitter. At least three of the Twitter users with whom Plaintiff had exchanged Direct Messages in 2015 were —highly prominent Saudi dissidents living outside of Saudi Arabia. At least three others, inside Saudi Arabia, were imprisoned after Plaintiff's text messages with them were stolen.

~~126.~~138. Fearing for his safety, Plaintiff withdrew from his studies and fled his residence, living in hotels for four months to avoid being kidnaped or harmed.

~~127.~~139. It was not until the publication of the October 20, 2018 New York Times article that Plaintiff learned that a suspected KSA agent had used the computer access Twitter had granted him to hack into Plaintiff's confidential information at Twitter.

~~128.~~140. Although Plaintiff's criticisms had already garnered attention from MBS and his allies it is highly probable that the combined effects of the disclosure of his private user information from Twitter and the spotlight shown upon him when McKinsey identified him as highly influential made him a much more prominent target.

~~129.~~141. In June of 2017, Loujain al-Hathloul, a feminist activist in Saudi Arabia, offered Plaintiff financial support and aid in getting a position with Amnesty International. In April of 2018 she was imprisoned and charged for her contacts with Plaintiff.

~~130.~~142. After defendants' misconduct, KSA's persecution of Plaintiff intensified to an unprecedented level. Between April and June 2017, an agent of MBS approached Plaintiff and said he had met with MBS. The agent attempted to convince Plaintiff to return to Saudi Arabia.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

This was during the same time period that MBS had tried to lure Dr. Saad Aljabri, back to Saudi Arabia to imprison, torture and/or murder him. Dr. Aljabri, a former high-ranking Saudi official, had become a prominent opponent of MBS.

~~131.~~143. From January 2018 to July 2018, Plaintiff had greatly restricted his social media presence, so the increased persecution inflicted upon him was more likely the result of KSA's increased intelligence on him.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75", No widow/orphan control

~~132.~~144. In mid-May 2018, two KSA agents contacted Plaintiff and asked to meet with him. Throughout a series of meetings with Plaintiff, they identified themselves as agents of MBS and said they were operating on orders from Saud Al-Qahtani, who was then a senior strategic advisor to MBS. The Central Intelligence Agency has concluded that MBS ordered Mr. Khashoggi's murder, and Al-Qahtani was the strategist who organized it.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

~~133.~~145. The two agents told Plaintiff that MBS was not happy with Plaintiff's political activities and criticisms against KSA in general and MBS in particular. The agents demanded that Plaintiff stop criticizing KSA and MBS and that he return to Saudi Arabia. Just as had been done with Khashoggi, the agents promised Plaintiff a bright future in Saudi Arabia. Plaintiff refused -both demands. When that failed the agents tried to persuade Plaintiff to come to the Saudi embassy in Ottawa with them. Plaintiff again refused. It should be noted that just a few months later, Mr. Khashoggi was lured to Saudi Consulate in Istanbul where assassins working for MBS murdered him.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

~~134.~~146. By the time Plaintiff refused to return to Saudi Arabia, KSA had significantly

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

increased its spyware capabilities. On information and belief, in 2017, KSA purchased or licensed the Pegasus spyware system from the Israeli cyber-spy company, NSO, for $55,000,000. This sum included NSO's technical support and training so that the Saudis would be able to use the Pegasus spyware.

~~135.~~147. On information and belief KSA was not able to deploy the Pegasus spyware until the Spring of 2018 at the earliest. Once the malware became operational to KSA, they acted. On June 23, 2018, Plaintiff's phone was infected by the Pegasus malware when he clicked on a link in a text message he had received. This was during the same period that Pegasus malware targeted and infected the smart phones of Dr. Saad Ajabri, and Ghanem Al-Masarir, another prominent Saudi dissident who was safely in the United Kingdom. Plaintiff was among the first Saudi dissidents KSA attacked with the Pegasus malware.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

~~136.~~148. Once the malware was downloaded to Plaintiff's phone it installed itself on Plaintiff's smartphone it exfiltrated all of Plaintiff's SMS chats, emails, photographs, location data, and other information to KSA. The Pegasus malware also enabled KSA to spy on Plaintiff in "real time", through control of his phone's camera and microphone, and through contemporaneous receipt of information Plaintiff typed into his phone or received from others.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

~~137.~~149. The intelligence gathered from Plaintiff's Twitter DMs and other private user data, coupled with Pegasus' uploading and transfer to KSA of all the data on Plaintiff's phone enabled Al-Qahtani and MBS to crush Plaintiff's family and his social network. In just a few short days between July 28, 2018 and August 3, 2018 the Saudi's rounded up and imprisoned both of Plaintiff's brother, and dozens of his friends, political allies, and even mere correspondents.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

~~138.~~150. Subsequently at the end of July 2018 and early August 2018, authorities acting on behalf of KSA increased their harassment campaign. KSA security forces raided Plaintiff's family home in Jeddah in the middle of the night using search dogs and conducted humiliating searches of the house. Two of Plaintiff's brothers were arrested and are still in prison without having been charged or receiving a trial. Security personnel acting on behalf of KSA have been torturing Plaintiff's brothers to pressure Plaintiff to stop his activism. According to a report by Amnesty International, such conduct is consistent with KSA security personnel's mistreatment of imprisoned activists.

~~139.~~151. During the first few days of his imprisonment, KSA security personnel would take Plaintiff's younger brother out of his detention cell and ordered him to call Plaintiff to beg Plaintiff to stop his political activities. They specifically mentioned the "electronic bees" project, which the Plaintiff worked on with the late Jamal Khashoggi and a small number of trusted close friends. That these KSA security personnel knew about Plaintiff's work to this level of detail was shocking to Plaintiff. At that point in time, Plaintiff had been unaware that KSA had been spying on him using the Pegasus system on his phone.

~~140.~~152. Plaintiff is informed and believes and thereon alleges that although Alzabarah invaded thousands of Twitter accounts of Saudi dissidents, KSA elected to use Pegasus malware to target only a relative few, including Plaintiff. Plaintiff is unaware of other Twitter users who KSA targeted with Pegasus malware. Plaintiff is informed and believes and thereon alleges that KSA targeted Plaintiff with Pegasus malware because of what KSA learned from accessing Plaintiff's Direct Messages on Twitter's platform that Alzabarah and Abouammo wrongfully accessed and furnished to KSA while Alzabarah was employed at

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Twitter, and because of the heightened scrutiny to which he was subjected by the McKinsey report.

~~141.~~153. Fearing for his safety, Plaintiff withdrew from his studies and fled his residence, living in hotels for four months to avoid being kidnaped or harmed.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

~~142.~~154. Dozens of Plaintiff's friends and associates who live in Saudi Arabia have also been arrested, tortured and subjected to inhumane and humiliating treatment even though most of them are not involved or even interested in politics. KSA security personnel have done this to pressure Plaintiff to stop his political activities.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

~~143.~~155. In mid-August 2018, Plaintiff was informed by Citizens Lab, which is part of the University of Toronto, that all of the information on his phone had been compromised by means of Pegasus malware.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

~~144.~~156. On October 2, 2018, Mr. Khashoggi entered the Saudi Consulate in Istanbul, Turkey, where he was murdered by an assassination team sent by KSA (specifically by MBS). Mr. Khashoggi, who championed democracy, human rights and anti-corruption efforts, had been a fierce critic of KSA.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

~~145.~~157. The collaboration between Plaintiff and Mr. Khashoggi had the potential to build a broad political movement for democratic reform in Saudi Arabia. Due to hacking Plaintiff's phone, KSA was aware of the collaboration between Plaintiff and Mr. Khashoggi.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

~~146.~~158. On or about October 15, 2018, less than two weeks after the extrajudicial murder

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

of Mr. Khashoggi, another team of Saudi nationals (known as the "Tiger Squad") traveled across the Atlantic Ocean from Saudi Arabia to Canada with the intention of assassinating Dr. Saad Aljabri and Plaintiff.

~~147.~~159. KSA agents continue to improperly pressure Plaintiff to stop his political activities with the help of Twitter, which recently suspended two of Plaintiff's Twitter accounts (@say_it_and_walk and @i5beearmy) without good cause.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

~~**TOS ISSUES**~~

TWITTER'S TERMS OF SERVICE

~~148.~~160. Twitter was available to anyone in the world who agreed to its Terms of Service (TOS). Plaintiff joined Twitter in October 2011.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

~~149.~~161. Plaintiff was required to assent to Twitter's Terms of Service (TOS)[5] as a condition of using Twitter. The terms "Services", "SMS", "API", "Transmissions" are not defined in the TOS. The TOS' exculpatory provision (labeled "Limitation of Liability") instructs users to use strong passwords: "Twitter cannot and will not be liable for any loss or damage arising from your failure to comply with the above." This would lead the reasonable reader to believe that Twitter treats loss of the password-protected private data as a special case, and that Twitter will not deny liability for the loss of private information so long as the user has reasonably strong password protection.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

[5] All references to the TOS are to the TOS applicable to the period in time where Twitter was negligent (2014-2015).

~~150.~~162. Twitter's website did not afford Plaintiff or any user the opportunity to negotiate with Twitter regarding the terms of the TOS, to offer to pay for greater security or removal of the TOS' exculpatory provisions. Twitter presented the applicable TOS to Plaintiff on a "take it or leave it" basis. Plaintiff was forced to either silence himself as a Saudi dissident by forgoing the most effective means of providing political commentary to the Saudi audience (see below) or risk damages from Twitter's negligence.

~~151.~~163. Although there is no monetary charge to use Twitter, it is not a free service because the user still incurs the cost of having their information mined and shared.

ALTHOUGH THERE ARE OTHER SOCIAL MEDIA PLATFORMS, THEY WERE / ARE NOT REASONABLE ALTERNATIVES FOR ACTIVISTS LIKE PLAINTIFF.

~~152.~~164. Although Saudi Arabia's population is smaller than California's, Saudi Arabia has the fifth highest number of Twitter users in the world.[6,7,8] Because of the tremendous popularity of Twitter among Saudis, there are a very great number of Saudis whom Plaintiff would not be able to reach with his messages unless he was on Twitter. A Saudi dissident who wanted to meaningfully reach a Saudi audience with political commentary must develop

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

---

[6] https://worldpopulationreview.com/countries Last visited Nov. 11, 2020

[7] https://worldpopulationreview.com/states Last visited Nov. 11, 2020

[8] 5 Social Media Trends in the Middle East in 2019 https://ijnet.org/en/story/5-social-media-trends-middle-east-2019 Last visited Nov. 11, 2020

a viable Twitter presence. Nothing compares to Twitter for Saudi activists. Twitter is seen by many analysts of the region as KSA's "only plausible free forum for political debate." [9]

~~153.~~165. Since 2011, most Saudis were shifting from Facebook to Twitter because the latter was geared more towards news on the Arab Spring. Public figures also started to create Twitter accounts. Plaintiff's voice and presence as a Saudi dissident would be heard better on Twitter than Facebook. For Saudis as of 2011, Twitter was a platform to spread political ideas while Facebook was useful to keep in touch with friends. Saudis viewed Facebook as more of a social platform, only interacting with their friends, whereas Twitter was seen as a political platform. If Plaintiff were to use Facebook, Saudis would not hear his voice. The impact of Facebook vs. Twitter in Saudi Arabia is also evidenced by Saudi officials and ministers having verified accounts on Twitter but largely ignoring Facebook. It was Twitter that was a key means of communication for protestors in the Arab Spring that threatened Saudi Arabia until KSA unveiled a populist $130 billion social spending package. From 2011, 2013, Facebook's market share in Saudi Arabia was sharply declining while Twitter's growth was exponential.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

~~154.~~166. Where Facebook allows a user to have no more than 5,000 "friends", Twitter provides for unlimited followers. Plaintiff presently has over half a million Twitter followers.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

~~155.~~167. Twitter also allows users to maintain their anonymity, which is a decided

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

---

[9] Alexei Abrahams, "Regional Authoritarians Target the Twittersphere", Middle East Research and Information Project, (Fall/Winter 2019). https://merip.org/2019/12/regional-authoritarians-target-the-twittersphere/ last visited November 11, 2020.

advantage for dissidents working against an authoritarian regime. Facebook, by contrast, requires users to register with their actual names. Even though Plaintiff tweeted in his own name, he also had a pseudonymous account to communicate with people who would not interact with his regular account. Activists frequently used Twitter's ubiquitous hashtag[10] (which are helpful in reaching relevant audiences) in the Arab Spring in 2011.[11] Facebook, however, did not introduce hashtags until 2015[12].

~~156.~~168. Further, Twitter is used for sharing ideas and keeping up to date with news and world trends, Instagram is intended to share a user's best photos and videos with their followers.[13]

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

POLICY ARGUMENTS

~~157.~~169. Policymakers in the United States are increasingly coming to the view long held

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

---

[10] "A hashtag—written with a # symbol—is used to index keywords or topics on Twitter. This function was created on Twitter, and allows people to easily follow topics they are interested in" https://help.twitter.com/en/using-twitter/how-to-use-hashtags. Last visited, Nov. 11, 2020.

[11] Alexei Abrahams, "Regional Authoritarians Target the Twittersphere", Middle East Research and Information Project, (Fall/Winter 2019). https://merip.org/2019/12/regional-authoritarians-target-the-twittersphere/ Last visited Nov. 11, 2020.

[12] Brent Barnhart, "How Hashtags on Facebook Still Work for Businesses." https://sproutsocial.com/insights/hashtags-on-facebook/ (January 22, 2020). Last visited Nov. 11, 2020.

[13] Caroline Forsey, "Twitter, Facebook, or Instagram? Which Platform(s) You Should Be On." (March 8, 2020) https://blog.hubspot.com/marketing/twitter-vs-facebook Last visited Nov. 11, 2020.

by European nations – that the internet in general and social media platforms in particular are too important to the public interest to be left unregulated or left to self-regulate:

A. Section 230 of the Communications Decency Act has already been amended to govern some content, and there are renewed calls in Congress to abrogate or limit the immunity social platforms such as Twitter enjoy from liability for the content posted thereon;

B. The Department of Justice has filed and is litigating an antitrust complaint against Google;[14] and

C. Facebook has been heavily criticized for amplifying and accelerating the genocidal campaign Myanmar military authorities have incited and carried out against Rohingya Muslims. Facebook is currently fighting an effort to subpoena its documents for a war crimes trial before the International Court of Justice.[15]

First Cause of Action Against Twitter, Inc., and Does 1-5 for Negligent Supervision and/or Retention of Employee

~~158.~~170. Plaintiff repeats and repleads each allegation in Paragraphs 1-~~157~~169 as though fully set forth herein.

~~159.~~171. Twitter hired Alzabarah and Abouammo.

~~160.~~172. Alzabarah and Abouammo became unfit and/or hazardous to perform the work

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

[14] https://www.nytimes.com/2020/10/22/technology/facebook-antitrust-ftc.html, Last visited Nov. 11, 2020) and https://www.nytimes.com/2020/10/20/technology/google-antitrust.html Last visited, Nov. 11, 2020.

[15] Application Pursuant to 28 U.S.C. §1782 v. Facebook Inc., Case 1:20-mc-00036 (D. D.C.)

for which they were hired.

~~161.~~173. Twitter knew or should have known that Alzabarah and Abouammo each were or each became unfit and/or hazardous to perform the work for which they were hired and that this unfitness and/or hazard created a particular risk to others including Plaintiff.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

~~162.~~174. As a direct and legal result of Alzabarah's and/or Abouammo's unfitness and/or hazard, Plaintiff has suffered emotional distress, loss of property and has incurred out-of-pocket expenses in excess of $75,000. Plaintiff had to move out of his apartment, withdraw from his graduate studies, and actually lived in hotels for four months.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

~~163.~~175. As a direct and legal result of Alzabarah's and/or Abouammo's unfitness and/or hazard, Plaintiff has also suffered stress, anxiety, emotional distress, pain and suffering, inconvenience, mental anguish, loss of enjoyment, and damage to personal and professional reputation.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

~~164.~~176. Twitter's negligence in hiring, supervising and/or retaining Alzabarah and/or Abouammo was a substantial factor in causing Plaintiff's harm.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Second Cause of Action Against Twitter and Does 1-5 for Negligence

~~165.~~177. Plaintiff repeats and repleads each allegation in Paragraphs 1-~~164~~176 as though fully set forth herein.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

~~166.~~178. By failing to design, evaluate, operate, modify, and/or maintain its security systems in a reasonably careful manner, Twitter was negligent. Further, by entrusting Alzabarah and Abouammo with the tools to gain access to Plaintiff's private user data, Twitter was negligent.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

~~167.~~179. As a direct and legal result of Twitter's negligence, Plaintiff has suffered emotional distress, loss of property and has incurred out-of-pocket expenses in excess of $75,000. Plaintiff had to move out of his apartment, withdraw from his graduate studies, and actually lived in hotels for four months.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

~~168.~~180. As a direct and legal result of Twitter's negligence, Plaintiff has also suffered stress, anxiety, emotional distress, pain and suffering, inconvenience, mental anguish, loss of enjoyment, and damage to personal and professional reputation.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

~~169.~~181. Twitter's negligence was a substantial factor in causing Plaintiff's harm.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 66 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Third Cause of Action Against Twitter, Inc. and Does 1-5 for Violation of California Penal Code § 502, et. seq.

182. Plaintiff repeats and repleads each allegation in Paragraphs 1-181 as though fully set forth herein.

183. By doing the acts alleged above herein Twitter has violated the California Penal Code § 502.

184. Specifically, Twitter has:

(a) violated California Penal Code § 502(c)(6) by knowingly and without permission, providing or assisting in providing a means of accessing Plaintiff's computer, computer system or computer network in violation of California Penal Code § 502.

(b) violated California Penal Code § 502(c)(7) by knowingly and without permission, accessing or causing to be accessed Plaintiff's computer, computer system, or computer network.

(c) violated California Penal Code § 502(c)(13) by knowingly and without permission, providing or assisting in providing a means of accessing Plaintiff's computer, computer system or computer network in violation of California Penal Code § 502.

185. California Penal Code § 502(e) provides Plaintiff the right to bring a civil action against Twitter for violations of California Penal Code § 502(c) for compensatory damages and injunctive relief or other equitable relief.

186. As a direct and legal result of Defendant's violation of § 502, Plaintiff has suffered damages in an amount according to proof at trial, but at least in the amount of seventy-five thousand dollars, plus the legal rate of interest.

187. California Penal Code § 502(e)(2) indicates that "In any action brought pursuant to this subdivision the court may award reasonable attorney's fees."

188. In bringing the present action, Plaintiff has and will continue to incur attorney fees and costs in a sum to be proven at trial.

189. California Penal Code § 502(e)(4) provides for the recovery of punitive or exemplary damages where it is proved by clear and convincing evidence that a defendant has been guilty of oppression, fraud, or malice as defined in subdivision (c) of Section 3294 of the Civil Code.

190. On information and belief, Plaintiff alleges that Twitter acted in conscious disregard of the rights and safety of plaintiff and of others, and otherwise acted in a manner that provided for the basis of imposing punitive and/or exemplary damages pursuant to California Penal Code § 502(e)(4).

192. Pursuant to California Penal Code § 502(e)(1), Plaintiff seeks injunctive relief to protect himself and future Twitter users from similar Twitter misconduct in the future. Specifically, Plaintiff seeks:

(a) A court appointed independent monitor, to be funded by Twitter, who shall regularly (at least once a month) audit Twitter's security operations and ensure that they include an adequate number of skilled and experienced professional investigators sufficient to monitor the conduct of Twitter employees who have access to confidential user data and assess when the conduct of any such employee may represent a risk to account holders. This monitor shall be ordered to report directly to Twitter's Board of Directors and the Court on a quarterly basis;

(b) Twitter shall develop and implement Monitor-approved policies and practices to ascertain whether Twitter employees are acting on behalf of a foreign government;

(c) When user accounts are breached or are the subject of an attempted breach Twitter shall timely report to users whether the breach is reasonably believed

to have been caused by a State-sponsored effort, and, if so, Twitter shall identify the State suspected to be involved; and

(d) When a Twitter employee or contractor views a user's IP address, telephone number, email address, activity log, or any information which would identity of the Twitter employee or contractor;

(e) When user accounts are breached or are the subject of an attempted breach by a person or persons whom Twitter reasonably believes may be or have been a Twitter employee or contractor, Twitter shall timely report to users and to the Monitor that the breach originated internally.

(f) Twitter shall install a security system that meets industry-level standards for protection of users private data, which would include human monitoring of alerts, require an employee who is trying to view private user data to apply for such access and show good cause before being able to view the private data and for such access to be granted only for a fixed time frame that is reasonably necessary for the employee to complete their necessary task and for that employee to only have access to the private user data that is necessary to complete the required task. Independent contractors would not have access to private user data under any circumstances.

(g) Twitter shall install a system that would be capable of actually enforcing its Playbook.

PRAYER FOR RELIEF

1. Compensatory damages for all economic loss, including but not limited to loss of past or future income, to the extent allowed by law.

2. General damages for pain, suffering, humiliation, and emotional distress to the extent allowed by law.

3. The costs of litigation, including reasonable attorney's fees, to the extent allowed by law.

4. Compensatory damages pursuant to California Penal Code § 502(e)(1).

5. For injunctive and prospective relief as the Court may order to prevent further wrongful acts, to the extent allowed by law.

6. Punitive damages and/or exemplary damages pursuant to California Penal Code § 502(e)(4) in an amount to be proven at trial.

7. For pre-judgment and post-judgment interest thereon at the maximum legal rate.

8. For such other and further relief as the Court deems just and proper.

DATED: ~~November 13, 2020~~April 19, 2021 RESPECTFULLY SUBMITTED

KLEIMAN / RAJARAM

By: /s/ Mark Allen Kleiman, Esq.

Mark Allen Kleiman, Esq.

LAW OFFICES OF BEN GHARAGOZLI
Ben Gharagozli, Esq.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial on all issues so triable.

DATED: ~~November 13, 2020~~April 19, 2021 RESPECTFULLY SUBMITTED

KLEIMAN / RAJARAM

By: /s/ Mark Allen Kleiman, Esq.

Mark Allen Kleiman, Esq.

LAW OFFICES OF BEN GHARAGOZLI
Ben Gharagozli, Esq.